CLAIMS

1. Method for user identification and ascertainment of authenticity of parties in a telecommunication system comprising:

a telecommunication network (OM);

a source system (LE1) connected to the telecommunication network (OM);

a target system (LE2) connected to the telecommunication network (OM);

said method comprising the steps of:

storing user identifiers and associated passwords in the source system (LE1) and in the target system (LE2);

logging on into the source system (LE1) by entering a user identifier and a password corresponding to it;

identifying the user in the source system (LE1);

setting up a remote session to the target system (LE2);

characterized in that in that the method further comprises the steps of:

generating identical indexed encryption keys in the source system (LE1) and in the target system (LE2);

encrypting the password associated with the user identifier in the source system (LE1) using the encryption key indicated by a first index, and sending the encrypted data as well as the first index and the user identifier to the target system (LE2);

encrypting the password associated with the user identifier in the target system (LE2) using an encryption key indicated by the index received;

performing a first comparison between the received password and the password encrypted in the target system (LE2);

encrypting in the target system (LE2) the password received from the source system (LE1) using an encryp-

tion key indicated by a second index, and sending the encrypted data and the second index to the source system (LE1);

encrypting the encrypted password initially sent from the source system (LE1) to the target system (LE2) again using the encryption key indicated by the second index received from the target system (LE2);

performing a second comparison between the encrypted password received from the target system (LE2) and the password encrypted in the source system (LE1) using the encryption keys indicated by the first and second indexes; and

approving the setup of the remote session if the results of the comparisons are coincident.

2. Method as defined in claim 1, characterized in that the setup of the remote session is prevented if the results of the first or the second comparison are not coincident.

3. Method as defined in claim 1 or 2, characterized in that

separate identification data is generated;

the identification data is encrypted in the source system (LE1) using the encryption key indicated by the first index and the encrypted data is sent to the target system (LE2);

the identification data received from the source system (LE1) is encrypted in the target system (LE2) using the encryption key indicated by the second index and the encrypted data as well as the second index are sent back to the source system (LE1);

the identification data encrypted using the encryption key indicated by the first index which was initially sent to the target system (LE2) is encrypted again in the source system (LE1) using the encryption key indicated by the second index received from the target system (LE2);

a third comparison is performed between the encrypted identification data received from the target

system (LE2) and the identification data just encrypted in the source system (LE1); and

the setup of the remote session is approved if the result of the comparison is coincident.

4. Method as defined in claim 3, characterized in that the setup of the remote session is prevented if the result of the third comparison is not coincident.

5. Method as defined in any one of the preceding claims 1 - 4, characterized in that

the identification data is sent simultaneously with the user data; or

the identification data is sent in separation from the user data.

6. Method as defined in any one of the preceding claims 1 - 5, characterized in that time data and/or data individualizing the source system is added to the identification data.

7. Method as defined in any one of the preceding claims 1 - 6, characterized in that the encryption keys are generated using a certain predetermined algorithm.

8. Method as defined in any one of the preceding claims 1 - 7, characterized in that the encryption keys are stored on a special encryption key list.

9. Method as defined in any one of the preceding claims 1 - 8, characterized in that the index is generated on a random basis or on the basis of a predetermined algorithm.

10. Method as defined in any one of the preceding claims 1 - 9, characterized in that a one-way encryption algorithm is used for the encryption of data in the source system (LE1) and in the target system (LE2).

11. Method as defined in any one of the preceding claims 1 - 10, characterized in that

the telecommunication system is a telephone exchange system.

12. Method as defined in any one of the preceding claims 1 - 11, characterized in that the source system (LE1) and/or the target system (LE2) are telephone exchanges.

13. Method as defined in any one of the preceding claims 1 - 12, characterized in that the telecommunication network (OM) is an operation and maintenance network.

14. System for user identification and ascertainment of authenticity of parties in a telecommunication system comprising:

a telecommunication network (OM);

a source system (LE1) connected to the telecommunication network (OM);

a target system (LE2) connected to the telecommunication network (OM);

in which system it is possible to store user identifiers and associated passwords in the source system (LE1) and in the target system (LE2), log on into the source system (LE1) by entering a user identifier and a password corresponding to it, identify the user in the source system (LE1) and set up a remote session to the target system (LE2);

characterized in that the system comprises:

means (1) for generating identical indexed encryption keys in the source system (LE1) and in the target system (LE2);

means (2) for encrypting data in the source and target systems using an encryption key indicated by an index;

means (3) for transmitting data between the source and target systems;

means (4) for performing a comparison in the source and target systems;

means (5) for approving the setup of a remote session.

15. System as defined in claim 14, characterized in that the system comprises means (6) for preventing the setup of a remote session.

16. Method as defined in claim 14 or 15, characterized in that the system comprises means (7) for generating identification data and adding time data and/or data individualizing the source system to the identification data.

17. System as defined in any one of the preceding claims 14 - 16, characterized in that the system comprises an encryption key list (8) for the storage of encryption keys.

18. System as defined in any one of the preceding claims 14 - 17, characterized in that the system comprises means (9) for generating an index on a random basis or on the basis of a predetermined algorithm.

19. System as defined in any one of the preceding claims 14 - 18, characterized in that the telecommunication system is a telephone exchange system.

20. System as defined in any one of the preceding claims 14 - 19, characterized in that the source system (LE1) and/or the target system (LE2) are telephone exchanges.

21. System as defined in any one of the preceding claims 14 - 20, characterized in that the telecommunication network (OM) is an operation and maintenance network.